CHAPTER

8

DESIGNING AN INTERNET CONNECTIVITY STRATEGY

After reading this chapter and completing the exercises, you will be able to:

- Understand the value of firewalls in an Internet connectivity design
- Understand the features of Microsoft Proxy Server 2.0
- Describe a functional Internet connectivity design using Microsoft Proxy Server 2.0
- Secure an Internet connectivity design
- Describe the major improvements provided by Microsoft ISA Server

In the last several years, dependency on Internet connectivity has expanded exponentially. Users within organizations now depend on Internet-hosted resources to accomplish their work, and organizations are offering services to their customers over the Internet. These businesses take advantage of a marketplace in which customers can buy goods and services all day, every day. In this chapter we will look at providing internal users access to Internet resources. In Chapter 9, we will explore the opposite—providing services to external users on the Internet.

We begin the discussion with firewalls.

Firewalls and Firewall Technologies

When an organization allows connectivity to the Internet or to a business partner's network, they open themselves up to a potentially huge security gap. Similarly, network connection between departments may expose security breaches in an organization, especially when one of those departments has extremely sensitive data. Therefore, network designers must include protection between the network (or portion of the network) and outside entities. These outside entities can be the wider world of the Internet, a partner's network, and even other departments in the organization.

The security solution, which is much more complex than it sounds, is a **firewall**. This term was borrowed from the one used in the construction trades to describe a wall built to prevent a fire from spreading between adjacent units in a building. A network firewall consists of both hardware and software. It protects a network from unauthorized access and from attacks from another network. A firewall controls traffic in both directions.

Firewall technology is ever changing because the world of interconnecting internetworks has grown more sophisticated and more dangerous. There are several basic types of firewall protection—often combined in the same product—but these technologies are constantly evolving to keep up with the imagination and skill of hackers. None of these technologies can stand alone as a firewall solution, but together, and with the value-added options given to them by various vendors, they provide firewall protection. We will look at each of these basic services in turn in the following sections.

IP Packet Filters

IP packet filters were added to routers to create the first firewalls many years ago. Such filters compare information found in the headers of packets and only forward packets that match a set of **rules**. For example, one rule could be to allow only connection attempts from within the private network; thus, the rule would reject any packets that contain connection attempts from outside. Another example could be a rule that eliminates TCP packets with destination ports on the internal network that are not supposed to be available to the external network. These destination ports might, for instance, be associated with NetBIOS shares. Presently, IP **packet filtering** comes in two types: stateless packet filtering and stateful packet filtering.

Firewalls that perform **stateless packet filtering** simply inspect IP packet headers and drop packets based on a comparison of information found in the packet header with rules. Such rules could involve source or destination addresses. Rules are enforced by the service associated with the rule. Stateless packet filtering ignores the state of the connection and myopically looks only at the individual packets. Figure 8-1 illustrates stateless IP packet filtering.

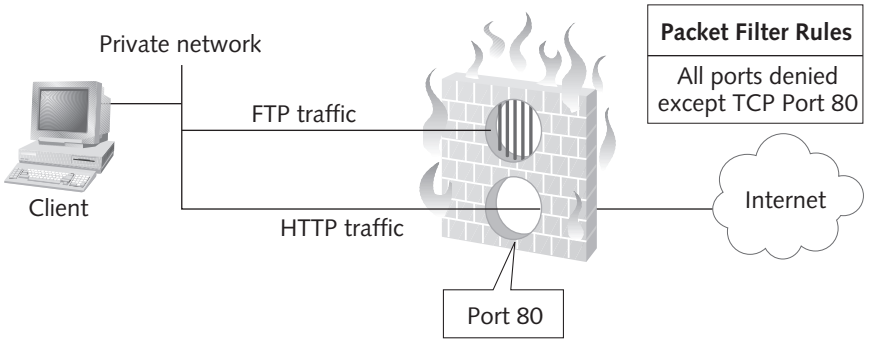

Figure 8-1 Stateless IP packet filtering

Both the TCP/IP packet filtering and the Routing and Remote Access Service (RRAS) packet filtering described in Chapter 7 are stateless. At one time, this function alone was adequate for firewalls, but various exploits, including IP address **spoofing**, made simple packet filtering, by itself, obsolete because it can limit addresses based only on the source IP address field of the header. (Spoofing replaces an address that would be rejected with one that the filter will allow to pass.) As we examine the other types of firewalls, you will see that IP packet filters alone would not protect your internal network.

Stateful packet filtering, also called **stateful inspection**, examines the payload of the IP packet and maintains a cache in memory of the state of the connections. Why are these features important? By examining the payload of a packet, stateful firewalls can detect packet data that could cause problems on the network and/or servers. For instance, malformed e-mail packets can be detected and dropped. Why is this important? Well, if these packets were allowed to reach an e-mail server, they could crash the server.

By maintaining information on the state of connections, firewalls that perform stateful packet filtering can detect when a connection to an inside resource is being attempted by an outside entity. If a return connection does not have a source address from the private network, it may be part of a hacking attempt such as a **denial of service (D.S.)**, in which a service is flooded with so many requests that it is too overwhelmed to handle valid ones.

Network Address Translation (NAT)

The **Network Address Translation (NAT)** protocol uses a method by which IP addresses on a private network can be hidden from external hosts through mapping to different IP addresses on the external internetwork. A single NAT-enabled computer placed between internal hosts and the Internet intercepts packets and modifies the source address in a packet. It maintains state information for this traffic so that when datagrams return, they are routed to the host that initiated the session. This provides transparent routing to the internal hosts, which do not have to be modified to benefit from NAT.

Figure 8-2 shows a client on a private network with the address 192.168.0.10. The client requests access to a Web page on an Internet server at the IP address A.B.C.D (sorry, we did not want to use a real address). The NAT server assigns a TCP port to the request, maintaining information about the internal address and the port to uniquely identify this request as being from the Web client at 192.168.0.10. It then maps this address and port to the translated address and port it uses in the destination field of the packet header when it sends the request to the Internet server. When the response comes back, it matches the response to the requests in the translation table and returns the request to the client.

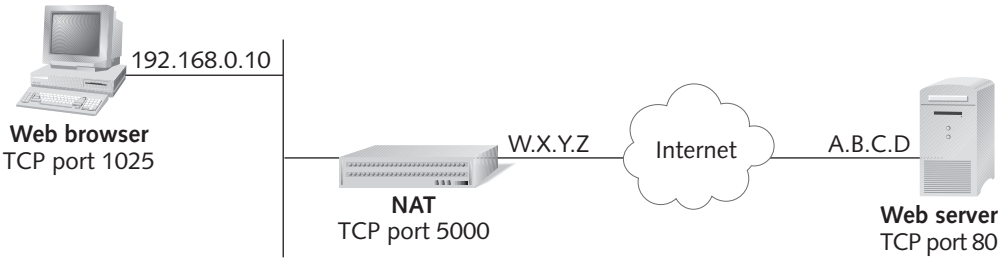

Figure 8-2 Network Address Translation

NAT allows an organization to have Internet access even when it does not have a registered address for every host that is given access to the Internet through NAT. In the properties of your external NAT interface, you may specify the pool of addresses your ISP has assigned to you for this purpose. Use the online Help function of Windows 2000 Server to learn more about NAT.

Life is full of limitations. There are limits to NAT as well:

- It only works when the applications do not use the IP addresses as part of the request itself. For example, NAT works well for Web browsing, because the connections are usually requested using DNS names rather than IP addresses. However, it does not work well with FTP because FTP uses IP addresses as part of the request itself.
- NAT is implemented in the TCP/IP stack, and as such it does not examine the contents of packets as an Application-layer component, such as a proxy, can.
- NAT cannot forward packets with encrypted TCP header information. These packets are the kind that might result from the use of an encrypted tunnel. A way to work around this is to have the NAT server (firewall) be the encryption endpoint.
- Because NAT changes the IP address information on packets, it interferes with software that uses TCP/IP address information for security checking. If a NAT implementation can inspect outgoing traffic for this type of security checking protocol usage, and if it maintains a translation entry to wait for the response, it is called service-specific NAT.

Rather than add functionality to NAT to get around its limits, NAT is usually combined with a service-specific proxy. Read on to see what proxies add to a firewall design.

Proxy Services

A **proxy service** works at the Application layer, intercepting outbound connection requests from internal hosts to external servers and acting as a stand-in for internal hosts. One enhancement to proxy services is **reverse proxy**, in which the proxy service is made available for external hosts accessing services on internal servers.

A proxy is also called an Application-layer gateway.

Whereas IP filters and NAT are completely transparent to the internal hosts, because they operate at the Network and Transport layers, clients using proxy services usually need to be configured to use them. For instance, Internet Explorer (IE) is configured to use Microsoft Proxy Server for Web browsing. Once configured, IE sends all requests to connect to Web sites to the Web proxy rather than attempting to make the connection directly.

Conversely, if your internal network is routed to the Internet and you are not filtering at the Network layer, a user can simply disable the proxy settings in IE to go directly to the network. Proxies that provide more security examine the content of the traffic for specific patterns, such as references in HTML pages to Java or ActiveX embedded applets, which could be Trojan horse-style viruses. The proxies then strip out such executable content.

A **Trojan horse virus** is disguised as a benign program. A user often "invites" a Trojan horse virus into their system by executing a program or embedded object in an e-mail that has an enticing name. Hackers who use Trojan horse viruses take advantage of human characteristics such as gullibility, lust, greed, and curiosity.

A **proxy server** may have proxies for several applications or types of applications, such as HTTP, FTP, and Telnet. With such Application-layer protection in place, you can completely block the flow of Network-layer protocols through the firewall and only allow these higher-level protocols through. In this way, you avoid hacker attacks on TCP connections in which the connection can be spoofed. We recommend that you use proxies for all applications, blocking the applications that are not authorized for your network and for which you do not have proxies.

There are a couple of caveats to working with proxies:

- For the best proxy protection, you must have a specific proxy for an application.
- Proxies alone are not effective protection; you still need to have the protection of IP filtering and stateful inspection, because users may bypass the proxy server if they can directly connect to the Internet without a proxy.

Circuit-Level Gateway

A **circuit-level gateway** works at the Session layer and controls internal traffic leaving the protected network. This is where rules such as allowable hosts and time limits are enforced, meaning that the traffic will be permitted or disallowed based on the parameters set in the rule. A parameter can be something such as the IP address of a host or the length of time for a session.

A session is the set of traffic between hosts over a networked connection that is managed as a unit for translation.

One circuit-level gateway, often considered a generic proxy, is **Socks proxy**, which can be used with virtually any TCP application, including Web browsers and FTP clients. The practical use of a Socks proxy is for services that do not have their own application proxy. In this case, the Socks proxy intercepts the packets and regenerates the packet while placing the original payload within the new packet.

The word "Socks" is derived from Sockets, a protocol used with TCP/IP to establish sessions through an identifier, also called a socket. A socket consists of an IP address and port ID, such as 192.168.20.3 and port 80, which indicate the HTTP service on the server at 192.168.20.3. WinSock—with which you might be familiar—is the name of a DLL that is the Microsoft implementation of Sockets for Windows. The disadvantage of a Socks proxy is that it does not examine the payload; however, just by regenerating the packet, it can avoid passing on malformed packets. As a proxy, it does hide the IP addresses of the internal clients.

Encrypted Authentication

When a firewall employs encrypted authentication, external users can be authenticated and authorized to open a connection through the firewall. Encryption protocols are used for this authentication. Note that this authentication is separate from encryption of the subsequent connection. Once authenticated, the user may perform all permitted functions on the internal net.

There are several disadvantages to encrypted authentication, including the following:

- The firewall must listen for and respond to connection attempts. This activity can make the firewall visible to hackers using programs that probe for just such behavior.
- Once established, an unencrypted connection could be redirected and misused.
- If a hacker captured the traffic during the establishment of a connection, it could spoof the address of the client after it is authorized, thus getting inside without needing to redirect the connection.
- Security keys stored on a notebook computer offer a special vulnerability. If stolen, this computer could provide entrée to the private network. There's a similar problem with users connecting from home, where an unauthorized person could use his or her computer to gain access.

- Windows NT encrypted authentication is generally not considered secure enough for use over the Internet.

Even with these disadvantages, encrypted authentication can still be effective if used carefully.

VPN Tunnels

Firewalls are ideal endpoints for a virtual private network (VPN) connecting two private networks over the Internet. When set up in combination with properly configured firewalls, a VPN is the safest way to pass information over the Internet. Using VPNs, users can address remote hosts at the destination private network by their private addresses, because the original packet becomes the payload of the packets in the encrypted tunnel. *Always use VPNs when connecting private locations over the Internet.*

Placement of Firewalls and the Use of Related Technologies

In your business and technical analysis, you determined the security needs of the organization. Like the "bricks and mortar" firewall, the placement of firewalls is determined by identifying what must be protected. You place firewalls at the connection points at which the security of a firewall is needed. For instance, look for the need for firewalls in the following locations:

- Between the private network and the Internet
- Between the private network and the networks of business partners
- Between departments within an organization
- At both ends of a slow WAN link in order to minimize traffic and enhance performance

The information that you gathered during the planning stage that affects your firewall design includes the following:

- Protocols, in use or planned, on the network (these will define the type of firewall and access method available to you)
- Server roles and services in use on the network
- Location of server roles and services
- User distribution in relation to the resources they require
- Definition of authorized and unauthorized traffic to identify what must be blocked, enhancing both security and performance
- Security needs of the organization

Now that we have examined firewalls in general, let's look at the intricacies of Microsoft Proxy Server 2.0.

GETTING TO KNOW MICROSOFT PROXY SERVER 2.0

Microsoft Proxy Server 2.0 is a set of services used to provide access to certain Internet services. It is beneficial to your network because, with it, you can allow users to have access to Internet services on another network while hiding users' or clients' actual IP addresses. You personally benefit from learning about Proxy Server 2.0 because the more you know about it, the more benefits you can derive from it.

We'll start our discussion with the feature set of Microsoft Proxy Server 2.0 and look at the services it offers. Then we'll look at the value of combining and integrating proxy services with other network services. Finally, we look at some of the issues surrounding the installation of Proxy Server 2.0.

The proxy server we use for our discussion in this chapter is Microsoft's Proxy Server 2.0 because Microsoft did not ship a new version of its proxy server when it released Windows 2000. Therefore, until the January 2001 release of the greatly enhanced proxy server replacement, Internet Security and Acceleration (ISA) Server, the Microsoft proxy server solution was Proxy Server 2.0. Because Exam 70-221 was created before ISA Server was released, ISA Server does not appear in the objectives for the exam. However, you can expect it to be included when and if the exam is updated. Therefore, we will include some introductory information about ISA Server later in this chapter.

Proxy Server 2.0 Features

Before we look at the individual services provided by Proxy Server 2.0, let's look at those features that Microsoft considers significant to a network design:

- It provides Internet access to authorized users through access control settings.
- It filters packets based on IP addresses and protocol port numbers, configured as one group of settings for all the client access services on a single proxy server. (Try Hands-on Project 8-2 to see the configuration options for access control and packet filtering.)
- It intercepts inbound Uniform Resource Locator (URL) requests and evaluates the traffic to determine whether it should be forwarded to an internal network resource (such as a Web server). This feature, known as reverse proxy, is one we will integrate into our network designs in Chapter 9.
- It provides **screened subnets** for added security. A screened subnet that is protected from a public network by a firewall may also be separate from the other subnets of the private network. Another term for screened subnet is DMZ (as in demilitarized zone).
- It provides enhanced performance for internal users accessing external resources through the interception of FTP and HTTP requests and the saving of retrieved objects in local cache.

Once Proxy Server 2.0 is installed, an administrator can use an MMC to manage it. Hands-on Project 8-1 walks you through the installation of Proxy Server 2.0, while Hands-on Projects 8-2 and 8-3 help you to configure Proxy Server 2.0 using the console. See Figure 8-3.

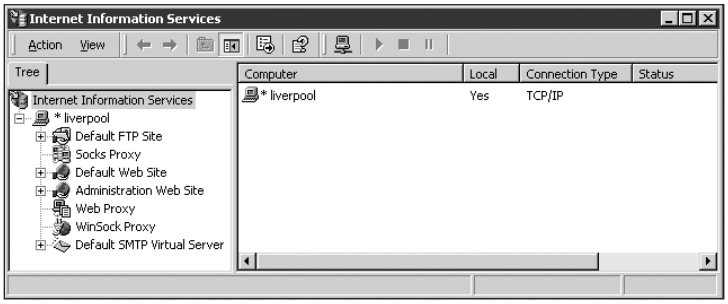

Figure 8-3 Proxy Server Management console

Proxy Server Services

There are several services and protocols included with Proxy Server 2.0, including Web caching, Web proxy, WinSock proxy, Socks proxy, and packet filtering. In the following sections, we will examine each in turn. As you go through the text, you will come to understand the differences between these services.

Web Caching

Proxy Server 2.0 caches Web pages it retrieves on behalf of clients. **Web caching** places only those objects accessed through the Web proxy service in the cache. It then checks its cache before retrieving the data on subsequent queries from clients. If the data is in the cache, Proxy Server 2.0 provides it from the cache.

Web caching can reduce the time it takes to provide pages to the clients, because they are being provided from the cache. This avoids going to the Internet to retrieve the page. Web caching only improves performance for a network design if there are many users repeatedly accessing the same sites.

You have your choice between active caching (the default) and passive caching. Both settings respond to client requests for Web pages. **Active caching** automatically updates the pages in the cache from their Internet sources based on both the number of requests for each page and the frequency at which it changes at the Internet source. Active caching takes advantage of times when processor utilization on the proxy server is low to avoid causing slower responses to client requests. When you disable active caching, the proxy cache service only retrieves Web pages when clients request them. This is known as **passive caching**. Active caching is configured on the Caching tab of the Web Proxy dialog box.

Plan on using Web caching for ordinary Web pages only, because secure Web pages cannot be cached. Adding additional proxy servers with separate Internet connections will enhance access to secure Web pages.

Web caching requires an NTFS partition on the proxy server machine. When you install Proxy Server 2.0, you will see the Microsoft Proxy Server Cache Drives dialog box, as shown in Figure 8-4. This allows you to select which drive to use. In Figure 8-4, the F drive is selected. We did this to illustrate that you want to select a partition other than the boot partition, which is what will be selected if Windows 2000 is installed on the C drive and that it is NTFS. We recommend that you select a drive other than the one containing the book partition because doing so can severely hurt performance. You also may select more than one drive for caches. Your own tests and actual client usage will vary, but a rule of thumb for setting the cache size is 100 MB plus 500 KB for each Web proxy user.

There are many settings for proxy server caching. For more details, see the Proxy Server Technical Notes and several Q articles, including Q259817, "How to Properly Configure or Modify Proxy 2.0 Caching Folders."

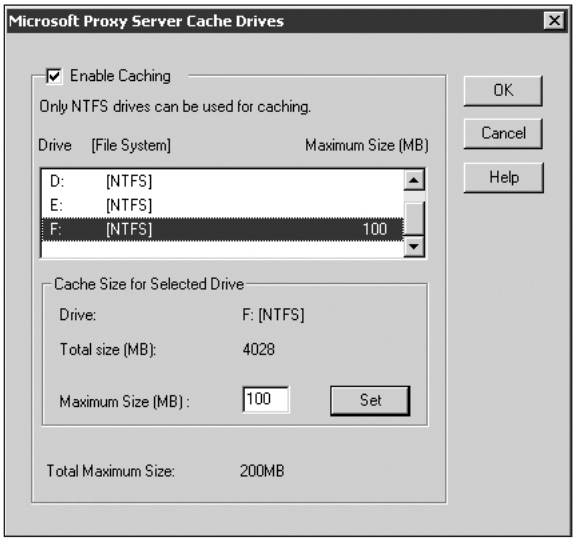

Figure 8-4 Proxy Server Cache Drives dialog box

This is not the end of the caching story—let's now talk about **distributed caching**, which allows you to distribute a cache across multiple proxy servers. There are two flavors of distributed caching in Proxy Server 2.0—proxy arrays (parallel structure) and proxy chains (hierarchical structure). Both use the cache array protocol (CARP).

Proxy arrays consist of two or more proxy servers that function in parallel to provide the caching service. They appear as one machine to the client, and each server contains separate cached data. The cache size of each proxy server is added to the array's cache. CARP lets the cache on each member act as part of a large cache. They provide a load-balancing function for Web caching. If one server becomes unavailable, the other servers continue to function.

Proxy servers in an array must be members of the same Active Directory domain, and all must be located in the same Active Directory site. CARP assigns a score to each URL before placing its data in the cache, and it uses this score to search for the URL the next time it is requested. If it is not found in the cache, the request is forwarded to the Internet. CARP maintains array efficiency as the number of servers increases, but there is a limit. A rule of thumb is to not exceed 20 servers in one array. Do your own testing and load analysis. Figure 8-5 shows a proxy array using parallel distributed caching.

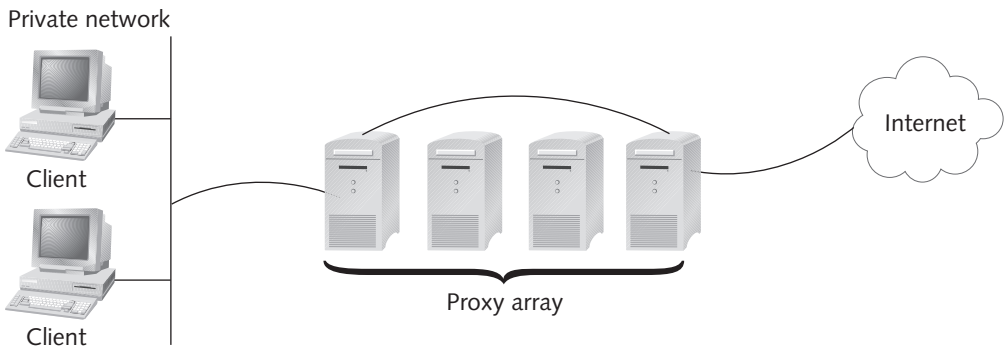

Figure 8-5 Parallel distributed caching

Proxy chains consist of a group of servers and/or arrays that work in a hierarchical structure (yes, arrays can be within a proxy chain). One server or array receives a request and, if it does not have the information associated with a URL cached locally, sends the request up the chain to the next "upstream" server or array. If that server or array doesn't have the Web page in its cache, it forwards the request to the next upstream proxy. The last server or array will send the proxy request to the Internet server hosting the URL.

You should consider using proxy chains for regional or branch offices that access the Internet through a central location. As illustrated in Figure 8-6, you can position proxy servers or arrays at each remote location and configure them to forward requests to a proxy server at the central location. Then, when a client in one of the regional offices requests a URL that is not cached in the local proxy cache, that server will forward the request to the central proxy. If the central proxy has the page cached, it will respond to the request, passing it back to the remote proxy. If the central proxy does not have the page in cache, it will retrieve it from the Internet and forward it to the remote proxy, which in turn will forward it to the client. The benefit of all this is increased performance

because cached pages will tend to be more available and won't have to be retrieved directly from the Internet.

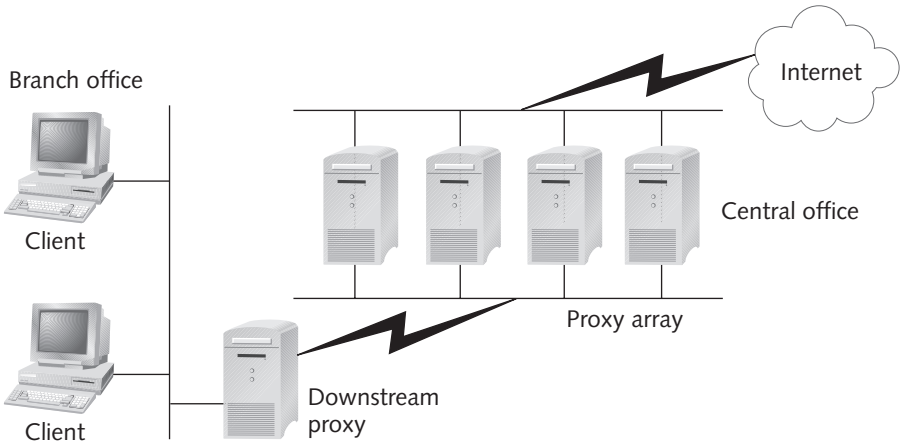

Figure 8-6 Hierarchical distributed caching

Web Proxy

The **Web proxy** service is an Application-layer gateway service that stands in for outbound connection attempts by Web browser clients, making the request to the Web server on behalf of the client and hiding the actual address of the Internal client. Web proxy responds to client Web browser requests using HTTP, HTTPS, and FTP. Web page caching enhances this service for clients. Access to the Internet through Web proxy is only given to client machines with a Web browser configured to use the proxy server.

WinSock Proxy

The **WinSock proxy** service is an Application-layer gateway. This service of Proxy Server 2.0 is available to clients with the WinSock proxy client installed. The WinSock proxy client can support any protocol that uses WINSock.DLL, including FTP, NNTP, Telnet, SMTP, POP3, RealAudio, HTTP, and HTTPS. WinSock Proxy can also be used by FTP when the client is not using a Web browser. It is installed with the Microsoft proxy client.

When windows authentication is required at the proxy server, you can use WinSock proxy for clients using the Netscape browser. It is important for your design that you understand how WinSock clients can be configured because the clients will fail to authenticate if they are not configured properly. From the Properties dialog box of WinSock Proxy, you can modify both the server and the client settings, which makes life easier because you don't have to touch every client computer. Modifications will be propagated to the clients the next time they restart or when the WSP program in Control Panel is run on each WinSock proxy client machine and the Update Now button is clicked.

Socks Proxy

The Socks proxy service is an Application-layer gateway used for client/server environments. It allows clients on one side of a Socks server to access servers on the other side of the Socks server through the Socks server. Its server component resides at the Application layer on the proxy server. The Socks client library resides on the client between the Application and Transport layers.

In order to provide secure communications between client and server computers, the Socks server authenticates and authorizes requests to connect to servers, establishes a proxy connection between itself and the server, and relays the data from the client.

Socks supports Telnet, FTP, Gopher, and HTTP, but, because it works at the Application layer, it does not support applications that require User Datagram Protocol (UDP), such as RealAudio, VDOLive, or Microsoft NetShow. You can use the Socks service for Macintosh and UNIX clients.

For more information on Socks proxy, point your Web browser to *www.socks.nec.com*.

Proxy Server 2.0 (and ISA, too) can have both a primary route and a backup secondary route to the Internet configured so that if the primary route is not available, the secondary route is used. When the primary route becomes available, proxy resumes the primary route. These routes can use a variety of access methods, and in your plans, you will want to assign the fastest connection to the primary route. For example, if you have two connections consisting of a T-1 and an ISDN connection, or an ISDN and a 56k dialup connection, you would choose the faster of the two.

Packet Filtering

Packet filtering is a Network-layer firewall function that allows only certain packets to leave or enter the local network. When you first enable packet filtering, Proxy Server's default packet filtering setting has all ports on the external interface closed. You must open specific ports to allow each type of traffic. This same set of filters applies to all three core proxy services of Proxy Server 2.0.

It is important to configure packet filtering to control traffic that will not be intercepted by the Application-level proxies. Such traffic includes the TCP, UDP, and ICMP protocols. Similarly, do not consider Proxy Server 2.0 to be a router. It will only pass packets recognized by its own Web proxy, WinSock proxy, and Socks proxy services.

Combining and Integrating Proxy Services with Other Networking Services

By now you are familiar with the modularity of Windows 2000 and the ease with which services can be combined and integrated. You might be asking, "What is the difference between combining and integrating?" Well, when services are combined, they are on the same computer. When services are integrated, they interact. That interaction can take place over the network or on the same box.

Combining and integrating are often discussed in the same breath because they are both considered ways to get more value from both the services and the hardware. They are both valuable options because both allow us to turn a computer into a multipurpose machine, thus getting more functionality out of the same box.

Some services should not be combined as a best practice, and other services cannot be combined in this sense. An example of services that cannot be combined are the DHCP service and the DHCP relay agent. They cannot be combined on the same computer because they use the same UDP ports. However, the DCHP service integrates well with the DHCP relay agent on the same internetwork, because the relay agent forwards requests from DHCP clients to DHCP servers, and vice versa.

When combining services, minimize the number of other services and applications you have on the server. In fact, treating the server as a dedicated proxy server is a very good idea. You don't want your proxy server to be forced to reboot just because a print spooler failed!

Nonetheless, several services can be combined, and we will talk about the special things you need to do in some cases. In addition, as we progress through the following sections, you will come to appreciate that integrating is an excellent idea, because it greatly enhances proxy.

We begin the discussion with Proxy Server 2.0 and IPSec.

Proxy Server 2.0 and IPSec

You can combine Proxy Server 2.0 and IPSec to provide authentication of communications and encryption of data sent over a public network. In Chapter 4, you perused several pages of information on using IPSec, so you are being spared a repeat here. Of course, we still want to say this: Test *everything* you hope to include in your design. This is especially critical if you are including IPSec because you may include an IPSec configuration that disables communications altogether.

Proxy Server and Routing and Remote Access

In Chapter 7, you examined the use of RRAS for WAN connectivity, so we will not go into detail here. However, we will say that Proxy Server 2.0 and RRAS can be combined to support nonpersistent connections. In this case, RRAS provides demand-dial connections for Proxy Server 2.0, as it did for WAN connections.

As mentioned earlier, Proxy Server 2.0 only passes packets for its own services. Theoretically, you can combine Proxy Server 2.0 and RRAS on the same server to have the benefits of a router, but it is a better practice to have them on separate boxes, placing the RRAS server at the connection point to the Internet, and the proxy server inside the private network. If you insist on combining them, be sure to turn on IP filtering. Otherwise, clients on the external network will be able to use the proxy server to access the internal network when you do not want to allow incoming traffic.

Proxy Server 2.0 and NAT

NAT is available with all Windows 2000 Server products through RRAS. NAT has three core functions that complement Proxy Server 2.0:

- It provides address translation of IP addresses and TCP/UDP port numbers of packets that are forwarded between the private network and the Internet.
- It provides IP addressing configuration information for DHCP client computers on the private network. This is provided by a simplified DHCP service, called the DHCP Allocator, that is part of NAT. It allocates IP addresses, the subnet mask, the default gateway, and the IP address of a DNS server to all DHCP clients on the internal network.
- It provides name resolution by a DNS proxy service. The service acts as a DNS forwarder, passing DNS requests to the Internet DNS servers for which it is configured, and returning the responses to the internal DHCP clients.

Although standard NAT translates the IP addresses in the IP header, the TCP port numbers in the TCP header, and the UDP port numbers in the UDP header, the Windows 2000 implementation of NAT includes NAT editors, which allow for translation using information beyond these three headers. Protocols, such as FTP, ICMP, PPTP, and NetBIOS over TCP/IP, that depend on IP information stored beyond these three headers do not normally work with NAT. However, the Windows 2000 NAT protocol has built-in NAT editors for all of these protocols and services. Furthermore, it has proxy software for H.323, Direct Play, LDAP-based ILS registration, and RPC. If your network design includes these protocols, you will be able to include NAT in your design.

NAT and IPSec are still like oil and water. NAT cannot properly translate IPSec traffic, so if you want to use IPSec in your design, the IPSec traffic cannot pass through a NAT router, but the tunnel can end at the NAT server.

With NAT you have some flexibility in configuring the NAT server, which is done through the RRAS console. First, you add NAT as a routing protocol through the General node of IP outing, as shown in Figure 8-7. At this point the protocol is installed, but it does nothing until you make it responsible for two or more interfaces.

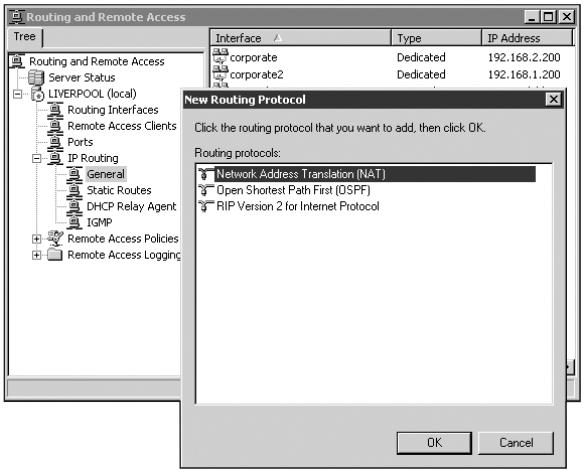

Figure 8-7 Adding NAT in Routing and Remote Access

You may add multiple interfaces to NAT, defining each as a "private interface" on the private network or as a public interface connected to the Internet.

Proxy Server 2.0 and Internet Connection Sharing

Internet Connection Sharing (ICS) is actually an implementation of NAT without configuration options. When you enable ICS, the interface on your internal adapter will automatically be given the IP address 192.168.0.1. You have no choice, which is appropriate when there are very few—perhaps less than 50—clients on the internal network. That is what ICS is for—very small private networks with no on-site support staff. For MCP Exam 70-221, you are coached to consider scenarios of 200 to 26,000 client computers, so you might think that ICS is completely out of the picture. However, you may well have small branch offices that connect directly to an intranet or the Internet and that would benefit from combining ICS and Proxy Server 2.0.

ICS is enabled through the properties for an Internet connection, as shown in Figure 8-8. The only configuration you may do to ICS is to specify the applications and services allowed over the shared connection. Those settings are accessed by clicking the Settings button on the Sharing page shown in the figure. Try Hands-on Project 8-4 for more information about this topic.

When you enable ICS, you will receive the warning shown in Figure 8-9. It describes the address that will be given to the internal interface. This is not configurable; it will act as a DHCP server for your clients on the internal subnet and act as a DNS forwarder for client requests. You only want to consider ICS for a very small single-subnet site.

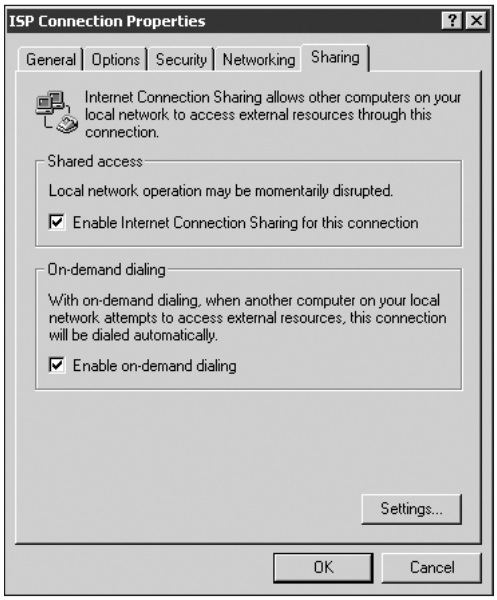

Figure 8-8 Enabling ICS

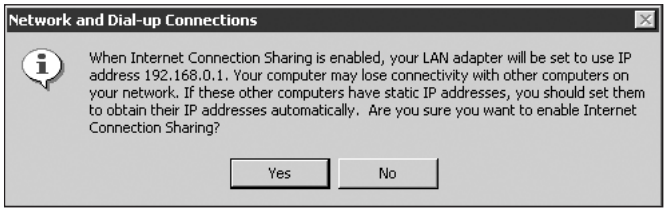

Figure 8-9 Warning about ICS

Proxy Server 2.0 and DNS

If DNS name resolution is needed on the internal network, you may install the DNS server on the same computer as Proxy Server 2.0, but there are certain cautions: You must disable the DNS service (not the client) for the external interface. This is done through the properties of the DNS server in the DNS console (see Figure 8-10), which has been configured to only listen for DNS traffic on the internal interface. You must make this change because the default configuration is "All IP Addresses," which is not what you want. Also, you must set file permissions on the HOSTS file on the server (if it exists) so that the file is inaccessible to Internet hosts.

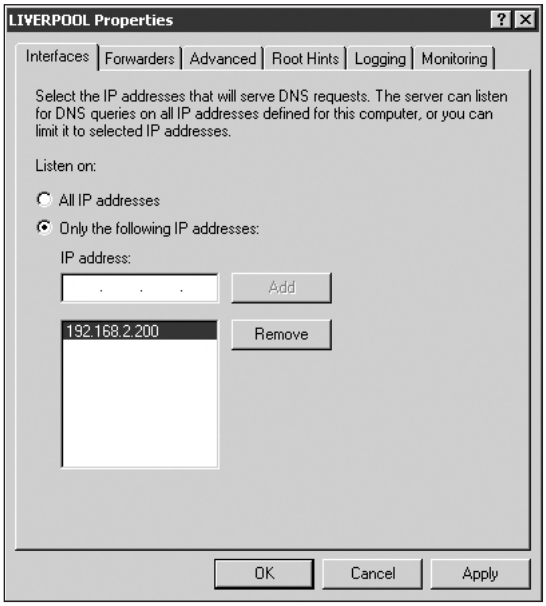

Figure 8-10 Disabling the DNS service on the external interface

If you are using multiple proxy servers, there are certain settings to which you must pay close attention. First, you must configure the TCP/IP properties of the internal adapter on each proxy server with the address of at least one DNS server (we recommend two for fault tolerance). Then, you must use DNS round robin for load balancing for inbound traffic. That strategy is discussed in Chapter 9.

Proxy Server 2.0 and WINS

We recommend that the proxy server be a WINS client if the internal network includes WINS servers. Also, if WINS services are needed on the internal network, you can add this service to Proxy Server 2.0, although there is one important precaution you must take to keep outsiders from discovering your internal NetBIOS resources. You must ensure that the internal adapter does not have a default gateway, and on the external adapter, you must disable the WINS client and deny Internet users access to the LMHOSTS file on the server.

For more information on configuring Proxy Server 2.0 with both WINS and DNS, see the Microsoft Knowledge Base Article Q257685, "Proxy Server 2.0 Security Checklist."

Installing Proxy Server

In order to run on a Windows 2000 server, Microsoft Proxy Server 2.0 needs Service Pack 1, and also must have some modifications made. The best, and recommended, way to successfully install Microsoft Proxy Server 2.0 on Windows 2000 is to use the Microsoft Proxy Server 2.0 Install Wizard for Windows 2000 (msp2wizi.exe), a special utility that can be downloaded from Microsoft's site.

To learn more about this, try Hands-on Project 8-1 for installing Proxy Server. Proxy Server 2.0 information can also be found in Microsoft Knowledge Base Article Q253131, "How to Install Proxy Server 2.0 on Windows 2000."

The Functional Internet Connectivity Design

Hey, you made it this far! Because you decided to stick around, we can now tell you how to create a functional proxy design to provide internal clients access to Internet resources. First, we will look at the business and technical objectives that will influence this design. Then we will look at the design considerations, including placement of proxy servers, an addressing strategy for the internal network, interface characteristics, and client-side configuration for proxy servers.

Your decision to use a proxy server will be influenced by the following business and technical considerations:

- Whether there is a user-by-user restriction on Internet and/or private network access
- Whether there is a resource-by-resource restriction on Internet and/or private network access
- Whether network configuration is routed or nonrouted
- Whether private network resources must be shared with Internet-based or extranet-based users
- Whether the private network includes multiple geographic locations

Your answers to these scenarios dictate the placement of, the planning for, the interface characteristics of, and the configuration of your proxy servers. We begin by discussing the placement of proxy servers.

Placement of Proxy Servers

Proxy servers, when part of an integrated firewall solution, are usually placed at the connection point between public and private networks to provide security and to keep traffic

local, in which case you are creating screened subnets. While this chapter has emphasized the "inside out" aspects of Internet connectivity, you should not look just at the perimeter of your private network for the placement of proxy servers, because there are opportunities to use proxy servers within the private network—either at connection points between networks or within a subnet.

We can explore this concept further by looking at proxy server placements at the perimeter of a private network, within a private network, and in the connection of dissimilar networks.

Using Proxy to Create Screened Subnets

Screened subnets come in different configurations. In all cases, a firewall-type device placed at the connection point between networks is controlling the traffic in both directions, with the security of one side of the connection as the top priority. The subnet on the "protected" side of the firewall is the screened subnet.

One type of screened subnet is the three-pronged screened subnet. In this scenario, the firewall has three interfaces—one connected to the Internet, one to the internal network, and a third connected to an internal subnet that has no connection to the internal network. (See Figure 8-11.)

You use such a subnet to provide access for incoming Internet traffic to Web servers, mail servers, and FTP servers within your private network. Only one subnet contains the servers that will be accessed from the Internet, and the network administrator will allow and restrict such incoming traffic using IP filters and reverse proxy. Conversely, the internal clients will be allowed access to Internet resources using appropriate proxy clients and IP filters. The internal clients can also be restricted to their use of proxy services with the use of user and group accounts either in Active Directory or in the local account database of a standalone proxy server.

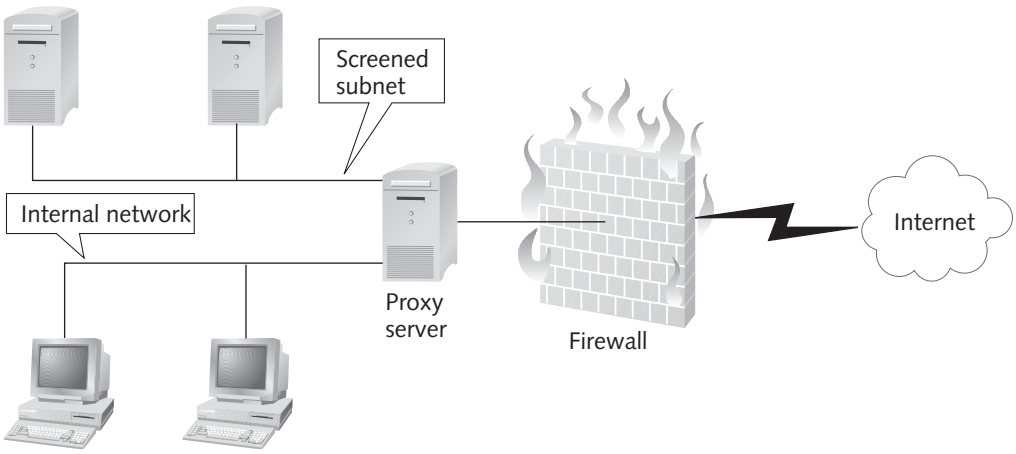

Figure 8-11 Three-pronged screened subnet

Another type of screened subnet can be positioned between subnets within the private network, with no direct connection on the proxy server to the Internet. For instance, in your network plan, you can place proxy servers between internal network segments so that Web pages are cached for network segments, thus reducing traffic within the private network. In addition, you can use proxy servers to create screened subnets between departments (on separate segments, of course) in order to protect confidential company data.

Using Proxy Within a Subnet

You might also consider *not* placing the proxy server at a connection point. When the proxy server is not positioned at the connection point between networks, it is simply a Web caching server. In this case, proxy clients on the internal network would send their Internet requests to the proxy server, which would send the requests through the router to the Internet. The proxy server then only needs a single interface—on the local network. Although this could produce more traffic on the subnet, it gives the clients the benefit of the proxy services, while keeping the proxy server behind the firewall.

Proxy Servers Between Dissimilar Networks

A Proxy server allows packets to be exchanged between dissimilar network segments, such as between the internal network's Ethernet segment and an ISDN, modem, or ATM segment. This makes it ideal to place at the edge of a private network. This placement, as you know, gives users on the private network access to the Internet and allows the Web pages to be cached for the entire organization. It also helps to isolate the private network from the Internet, thereby giving additional protection.

Planning for Internal Network Addressing for Proxy Services

Because proxy services make Internet requests on behalf of internal clients, the packets sent to the Internet contain the source IP address of the proxy server, not the client that actually made the request. You will want to consider the current IP addressing usage to see if it needs to be altered before implementing Proxy Server 2.0. If the clients were previously routed to the Internet, they had public addresses, unless NAT was employed for address translation. Note, however, that using public addresses for proxy clients can be wasteful and expensive.

Internal network addressing is critical to your design because you may discover some cost savings by replacing a range of leased Internet addresses with private Internet addresses that can be used for free. When planning for the use of Proxy Server 2.0 in your network, evaluate your current IP addressing strategy to see if it should be changed. In addition, consider the nuances of addressing strategies.

Addressing Strategy—Private Versus Public IP Addresses

When possible, you should use addresses on your internal network that, if they become known to outsiders, cannot be used from the Internet. Private Internet addresses should be used for hosts; hosts should not have their addresses visible on the Internet.

Internet routers are configured to drop all packets coming from or going to the private network addresses. This provides at least a modicum of security. Also, it is expensive to lease public IP addresses, and they should not be wasted when the addresses are not going to actually be used on the Internet, as would happen when a client uses Proxy Server 2.0 to access the Internet.

The Local Address Table

The **Local Address Table (LAT)** is a list of internal subnet addresses. It is maintained by the proxy server and is a critical component because it is the proxy's routing table.

You do not configure the internal interface on Proxy Server 2.0 with a gateway, because you want Proxy Server to use its LAT to determine which IP addresses are on the local network and which are on the external interface. When the proxy server receives a packet, it examines the LAT to see if it contains the destination address. If it is there, the proxy server forwards the packet to the local network. If the address is not there, the proxy server sends the packets to the external network. These addresses are shown in the LAT in pairs, as illustrated in Figure 8-12.

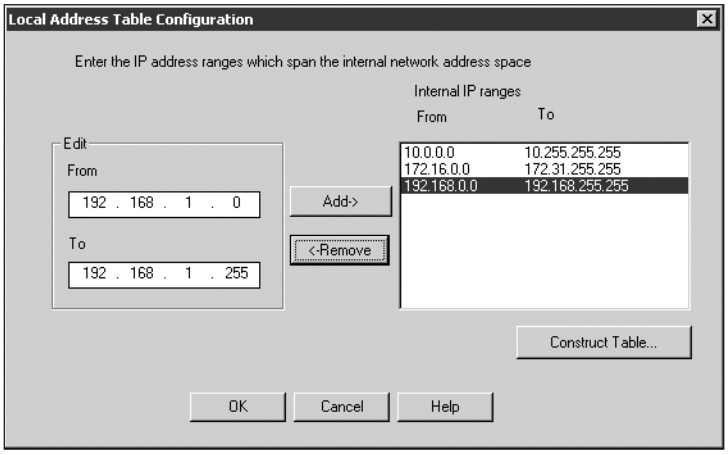

Figure 8-12 Configuring the LAT for Proxy Server 2.0

You can configure the LAT during the installation of Proxy Server 2.0, and you can configure it after the fact from the management console that we mentioned earlier. You can manually create the LAT, or use the Construct Table button during the installation of

Proxy Server 2.0. In the latter case, it uses the private ranges defined by the IANA as well as the address ranges it discovers.

When planning for internal network addressing, be sure that the LAT does not contain any Internet address ranges. If it does, traffic from the internal network that is sent to those addresses would never make it to the Internet, because the proxy server will believe that those addresses are on the private network.

Interface Characteristics

A proxy server with just one interface can be used for Web caching. When it is positioned at a connection point between networks, however, it must have two interfaces. Each interface must have TCP/IP bound to it and must have an IP address and a subnet mask.

The IP address and subnet mask on an internal interface must be congruent with the internal segment to which they are connected. In addition, you must make decisions about using public or private addresses on the internal network. Because the proxy server hides the client from the external network (the Internet), the internal network can use addresses from one of the private ranges that (officially) is not routed on the Internet and not accessible directly from the Internet.

The network segments to which Proxy Server 2.0 connects can be persistent or non-persistent, and they can vary between network segments, based on the needs of the design. Note that when the external network segment is a LAN technology, you should include a demand-dial interface with a VPN in order to exchange credentials for the connection.

You might feel that Web caching falls under the category of a performance enhancement, but this is perhaps the main motivation for using a proxy server; so consider it part of a functional design. However, recall that the principal value of Web caching depends on having many users frequently accessing the same Web pages.

Client-Side Configuration for Proxy Server

Client-side configuration is important to understand so that your clients will get the protection and performance benefits of Proxy Server 2.0. It is important for designing Internet connectivity because without the correct client configuration, your clients will be unable to receive the greatest benefit in both security and performance.

Before you can appreciate the nuances of client-side configuration for Proxy Server 2.0, you need a little history lesson and examination of the behavior of Internet applications such as FTP, WWW, and Gopher. This information is important because selecting the correct client configuration depends on knowing the applications and services the client needs to run.

FTP, WWW, and Gopher are client/server applications and use client-to-server communication standards established as part of HTTP as far back as the invention of the World Wide Web and the first programming libraries that supported it. The folks at CERN added support for proxy services to their libraries, which were adopted as standards by the WWW community, which then led to the term "CERN-compliant." CERN-compliant Web proxy services support WWW (HTTP/HTTPS), FTP, and Gopher requests, but all communication between the client and the proxy server is through HTTP. Proxy Server 2.0 includes a CERN-compliant Web proxy.

CERN is the French acronym for the European Organization for Nuclear Research. In the 1980s, CERN was an early adopter of the TCP/IP protocol suite for their network, CERNET. In 1990 a computer scientist at CERN, Tim Berners-Lee, invented the World Wide Web. Learn more about CERN at *http://cern.web.cern.ch* and read about the CERN standards at *www.w3.org*.

Proxy Server 2.0 has client software, but it may not be necessary to install this on all your client computers. Whether you use the client software depends on your requirements. In your Proxy Server 2.0 network design, you have four choices for client-side software. These include Microsoft Internet Explorer 5.0, Proxy Server Client, Socks, and no client at all for clients that don't qualify for other options.

Microsoft Internet Explorer

Microsoft Internet Explorer 5.0 (IE 5.0) is your choice for HTTP and FTP traffic and for any operating system that can run Internet Explorer. It runs only on TCP/IP and benefits from the server-side Web proxy configuration of outbound and inbound packet filtering and outbound domain filtering. IE 5.0 can be configured to automatically detect a Web proxy server, so it doesn't need individual configuration at the workstation when changes are made on the proxy servers. You can change settings on the Connections tab of IE's Internet Options dialog box.

The Web proxy service of Proxy Server 2.0 is compatible with CERN proxy but is a separate service. Web proxy is accessed by a separate protocol from the client, whether the client is doing FTP, HTTP/HTTPS, or Gopher.

Proxy Server Client

The Proxy Server Client supports any operating systems that support WinSock. Proxy Server Client has a copy of the proxy server's LAT, and it forwards to the proxy server only those packets that are destined for remote network locations. This is your only choice if your internal network is IPX/SPX. The Proxy Server Client benefits from the server-side configuration of protocol rules and packet filtering.

Socks

This is your choice for UNIX and Macintosh clients, and for operating systems that run Socks-compatible applications. The Socks client benefits from the server-side setting of protocol and Socks rules and IP packet filters. Socks client software does not come with Proxy Server 2.0, but it can be downloaded from ftp://ftp.nec.com/pub/socks. You will need version 4.3a, which is supported by Proxy Server 2.0.

No Client

This may be your choice if you do not need to support IPX/SPX-based internal networks or you do not have UNIX, Macintosh, or other clients running Socks-compatible applications. Without a Proxy Server Client, you need to configure the client default gateway to point to the IP address of the proxy server.

Unfortunately, this has a downside: Traffic not intended for the local subnet will be sent to the proxy server, which will forward it to an internal router. Obviously this will cause more traffic. However, the client traffic will still be controlled by proxy protocol rules and IP packet filters.

In your travels, you might see references to the use of CERN-compliant clients without a WinSock proxy. Such clients, if configured with a proxy server/IP port, will use the proxy service without the WinSock proxy client installed. However, in your planning, note that these clients do receive the benefit of caching. Alternately, non-CERN-compliant clients can be configured with a default gateway pointing to the proxy server; then the client can still have the packet filtering and forwarding benefits of Proxy Server 2.0, but no performance benefits, such as Web page caching.

Securing a Proxy Server Design

There are several strategies Microsoft recommends for securing a proxy server design. These security methods can include the requirement to have authenticated access through Active Directory and limiting access to sensitive internal data and Web sites. Regardless of the methods used, they have one goal—security. We discuss additional nuances of security next.

Restricting User Access to the Internet

You may restrict user access to the Internet through Proxy Server 2.0 with or without an Active Directory domain. Let's first look at the options available to you if you do have an Active Directory domain. With an Active Directory domain, you can grant Internet access to users and groups in Active Directory. The following provides a guide of the accounts to use based on the access you wish to provide:

- To grant access to all users, regardless of whether they are authenticated, enable the guest account on the proxy server and give permission to the group Everyone.

- To grant access to groups of users, organize the users into Active Directory groups and give permission to those groups.
- To grant access to individual users who have Active Directory accounts, simply select the users and grant them access.

If you do not have an Active Directory domain, you have several choices. All of these choices assume that Proxy Server 2.0 is installed on a standalone Windows 2000 server:

- Create local user group accounts on the server.
- Use utilities to replicate accounts from other network operating systems into the local accounts database (the SAM) of the proxy server. Novell has software that will allow you to do this.
- Allow anonymous access to the proxy server by enabling the Guest account on the proxy server and granting proxy server access.

Using Screened Subnets

Through your business and technical analysis, you have determined the security requirements for your design. This will guide you in deciding where to place screened subnets. Create a screened subnet in any location where you need to control traffic using IP packet filtering, Web proxy, Socks proxy, or WinSock proxy. Once you have determined the location of screened subnets, you will need to determine the number of proxy servers required to create the screened subnets.

Figure 8-11 showed three subnets, each connected to a different interface on a single proxy server. You could also have three screened subnets, each with a separate proxy server. The following points will help you choose multiple interfaces in a single proxy server, as in Figure 8-11, or in multiple servers:

- Choose multiple interfaces if the single proxy server can handle the expected traffic and processing load for the multiple interfaces and the organization has a centralized administration model.
- Choose multiple servers if the traffic and processing load require a dedicated server on a subnet and if the organization has a decentralized administration model.

If your design requires multiple screened subnets using multiple proxy servers, you will need to place the proxy servers in a hierarchy if you wish to do the following:

- Delegate administration of the proxy server and the subnets it serves, because a hierarchical arrangement allows you to have a centralized administrator at the top who grants permissions to the servers lower in the hierarchy to other support personnel.

- Centralize the establishment of security. The security at the top is the minimal security that will be applied to the entire hierarchy.
- Establish stronger security lower in the hierarchy; you can always make your security more restrictive further down. It will do you no good to loosen restrictions down in the hierarchy, since the top of the hierarchy is "guarding the door."

Using IP Packet Filters

Traffic can be restricted between the private network and the Internet through the use of packet filters. Packet filtering can control all IP traffic regardless of the proxy services in use. In addition, it can control all inbound and outbound packets.

Packet filter criteria can be combined on each interface through the use of multiple filters. These criteria include the following:

- Inbound, outbound, or both directions
- TCP, ICMP, or any Protocol ID
- Local port, which is the TCP or UDP port number for the source if the packet originates in the private network, or the destination if the packet originates outside the private network
- Remote port, which is the TCP or UDP port number for the destination if the packet originates in the private network, or the source if the packet originates outside the private network
- Local host IP address, which is the IP address of the host on the private network exchanging IP packets with the remote computer on the Internet, which is usually the proxy server
- Remote host IP address, which is the IP address of the remote computer on the Internet that exchanges IP packets with the computer on the private network

Using Domain Filters

There are situations in which you are asked to restrict the Internet resources to which users connect. This requirement may be for security reasons, for performance reasons (limiting traffic), or to prevent liability from harassment activities of employees accessing Web sites that are offensive to their co-workers. Proxy Server 2.0 allows an administrator to restrict the Internet resources that internal clients may access through the use of **domain filters**, which work at the Application layer to allow or deny access to Internet sites, based on IP address/subnet mask or domain name.

Domain filters apply to clients of Socks proxy, Web proxy, and WinSock proxy. Domain filters for Web proxy and WinSock proxy can be added through the Proxy Server 2.0 management console in the Properties dialog box of any of these services. Once you are

one of these dialog boxes, you must click the Security button, and then select the Domain Filters tab. Then you put a check mark in the Enable Filtering box, and you have some decisions to make. If you select the option button labeled Granted, then access is granted to all Internet sites except those you list in the box. If you select the Denied Option button, then access is denied to all Internet sites except those you list in the box. Further, a domain filter can filter on a single computer (single IP address), group of computers (range of IP addresses), or fully qualified domain name (FQDN). You may have several domain filters to create the restriction required for the design. Note that domain filters for Socks proxy must be added through the Permissions tab of the Socks Proxy Service Properties dialog box.

So how would you use domain filters? Consider an organization that allows Internet accesses exclusively for access to a few sites that are critical to the operation of the business, and they want to discourage Internet access for any other purpose. In this case you would design a set of domain filters to deny access to all Internet sites except those few sites required by the business needs.

Here's another scenario: Consider an organization that allows employees to access a wide range of Internet sites, but that has a policy against access to a list of sites they consider offensive in the workplace. In this case, you allow access to all sites except those on the list. An organization that feels compelled to do this will also find that their list grows; so plan to make regular updates to the domain filters.

Enhancing a Proxy Server Design for Availability

A design that has a single proxy server at any junction between networks has a single point of failure. This single server could be overwhelmed with the traffic and processing involved, which puts it at risk. Also, if the single server fails for any reason, the flow of traffic stops. For this reason, it is important to consider using proxy arrays to avoid this single point of failure. To use an array, there are only two requirements:

- All servers that are members of a proxy array must be members of the same Active Directory domain and site.
- All servers that are members of a proxy array must use the same proxy array name.

They are rather simple requirements for the benefit you will derive. When you set up the array and configure the caching settings, you will achieve some performance enhancement if you have many clients accessing the same Internet sites over and over again. This is a very specific limit to the performance enhancement. But you will also receive the availability enhancement of failover. Failover occurs when a proxy server that is a member of an array fails, and the other members take over the handling of client requests.

Enhancing a Proxy Server Design for Performance

There are several options for enhancing a proxy server design for performance. When you are using a single server, make sure that you have the best hardware for the job. Because of the Web page caching and the network interface handling all the traffic, proxy services severely tax the hard disk subsystem. So, you should use a fast disk subsystem and high-quality server NICs in the proxy servers.

Whether you have single proxy servers at each location or multiple proxy servers, you should enable caching if there is any chance that users will benefit from the caching of Web objects. Remember that you will derive the greatest benefit from caching in a situation in which many users access the same site over and over again—although you will still have some benefit in a situation in which it is less likely that this condition exists. When you enable caching, you have the following choices:

- Turn on caching with the default of active caching in order to reduce Internet traffic and have the cached Web objects updated when processor utilization on the proxy server is low. This makes it more likely that the current Web object will be in the cache when the user requests it.
- Turn on caching, but disable active caching (which enables passive caching) in order to save on system resources. However, this means that Web objects are only retrieved at the time the user requests them. An object cached at the last request is more likely to be outdated.

Beyond these simple caching settings, if you have multiple locations going through a central site for Internet access, you should consider configuring hierarchical distributed caching. The proxy server or arrays at the remote locations can manage caching for that site. The number of users at each location will help determine the need for a single proxy server or an array of proxy servers. At remote locations, configure the array or single proxy server to forward proxy client requests to the server or array at the central office, which will search its cache for the Web object. Then, you can forward the request to the Internet if it does not have the object in cache.

Internet Security and Acceleration Server—the Next Big Thing

Many were disappointed when Windows 2000 was introduced without an upgrade to Microsoft Proxy Server 2.0. However, in January 2001, Microsoft introduced Internet Security and Acceleration (ISA) Server as the next version of this product. The new name reflects its new position as a standalone Internet security product—a firewall. It now supports more protocols and does not rely on the installation of client-side software to benefit from proxy services.

ISA Server comes in two flavors:

- ISA Server Standard Edition is a standalone product that uses local policy and supports up to four processors. It has limited scalability, limited Active Directory integration, and hierarchical caching.

- ISA Server Enterprise Edition is a multiserver product with centralized management, no limit on the number of processors supported, and support for enterprise and array policies. It provides full scalability, both distributed and hierarchical caching, full Active Directory integration, tiered policy support, and multi-server management. This version fully integrates with Active Directory. To do so, it requires a schema-modification procedure before it can install in Enterprise mode. This procedure is called ISA Server Enterprise Initialization. This must be run by a member of the Schema Admins group and is *not reversible*.

Both products require Windows 2000 Server or Windows 2000 Advanced Server, but both can be installed in a standalone configuration for networks without Active Directory.

ISA Features

ISA Server now can compete with many firewall products, because in addition to the packet filtering, circuit-level filtering, and application-level filtering capabilities of Proxy Server 2.0, ISA now supports stateful packet filtering. It can also provide security for individual features and services at the user or group level using Active Directory or Windows NT SAM accounts.

ISA Server provides NAT services through its SecureNAT feature, which allows hosts to benefit from both the NAT and firewall services simply by having their default gateway point to the ISA Server. No special client software is required for this. However, you will want to install ISA Server's firewall client to gain the following benefits:

1. The ability to apply rules to user names and groups rather than client IP address
2. The automatic configuration of client browsers to use the firewall server, although you can configure this manually if you choose not to install the firewall client

In addition to these firewall features, ISA offers improvements to the caching capabilities of Proxy Server 2.0 and **intrusion detection,** which is the monitoring of activity that would indicate hacking. ISA Server is a huge product. Many books are being written about this one product, and careers are being enhanced and built around this and other firewall products. One look at the ISA management console, shown in Figure 8-13, tells you this is a very complex product.

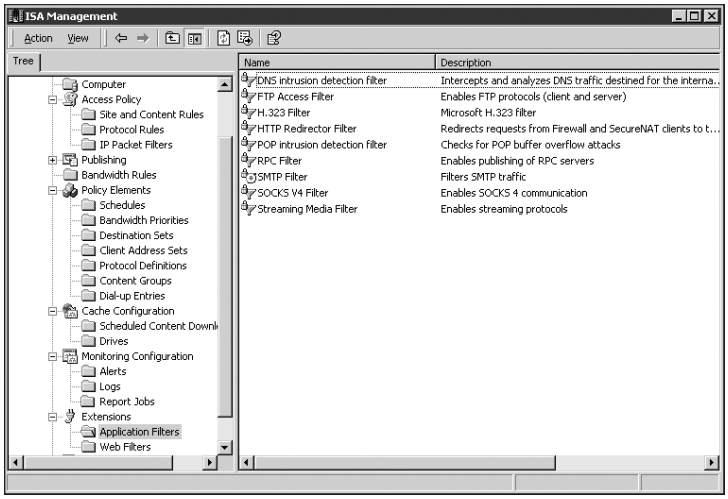

Figure 8-13 ISA Management console

To learn more about ISA Server, direct your Web browser to *www.microsoft.com/isaserver*.

Chapter Summary

- In this chapter, we examined Internet connectivity design options. This is an important area of network design because the need and desire to have Internet access while on the job has increased many times over, especially since the advent of the World Wide Web. Five to six years ago, companies requiring Internet access for their users were in the minority. Now it is very common for Internet connectivity to be a business requirement for a network design.
- With Internet connectivity comes a special set of problems and requirements. This connection to the untrusted (and perhaps untrustworthy) environment of the Internet presents serious security problems. Internet hackers are finding more and more ways to break into private networks to cause mischief and even to sabotage and steal data. The solution is to use a firewall. We looked at the generic functionality of firewalls, but based our design considerations on the firewall and proxy capabilities of Microsoft Proxy Server 2.0.
- We know this is probably a bad idea because both hacker and firewall technology has been moving so fast since Proxy Server 2.0 was created. We use Proxy Server 2.0 for two reasons. One is that this book is a test preparation guide for a Microsoft exam. Second, their much more capable product, ISA Server, was not available when the exam was written and, therefore, is not yet included on the exam objectives. We do include a look at the ISA Server features in Chapter 9, because that is

where we can show off its features the best—protecting internal servers as external clients are accessing them.

- After justifying inclusion of Proxy Server 2.0 in this chapter, we considered its features, provided through such services as IP filtering, Web caching, Web proxy, WinSock proxy, and Socks proxy. We considered the merits of using private Internet addresses on the internal network versus public Internet addresses and followed that with examination of the function and configuration of the Local Address Table (LAT).
- We considered the value, capabilities, and dangers of combining Proxy Server 2.0 and other network services on the same server. You had an opportunity to consider the types of clients you need to include in your plan based on the operating systems, applications, and protocols running on the client computers. The chapter concluded with a discussion of how to arrive at a functional Internet access design.

KEY TERMS

active caching — Automatically update the pages in the cache from their Internet sources based on the number of requests for each page and the frequency at which it changes at the Internet source.

circuit-level gateway — A session-layer protocol that uses rules to control internal traffic leaving the protected network.

denial of service (D.S) — A hacking method in which a service is flooded with so many requests that it is too overwhelmed to handle valid ones.

distributed caching — Allows you to distribute a cache across multiple proxy servers.

domain filters — Filters that work at the Application layer to allow or deny access to Internet sites based on IP address/subnet mask or domain name.

firewall — Used to protect a network from unauthorized access and from attacks from another network. A firewall controls traffic in both directions and consists of both hardware and software.

intrusion detection — An ISA improvement that monitors activity that would indicate possible hacking.

Local Address Table (LAT) — A list of internal subnet addresses maintained by the proxy server, which is actually the routing table of Proxy Server 2.0.

Network Address Translation (NAT) — A protocol that is used to hide IP addresses on a private network from external hosts through mapping to different IP addresses on the external internetwork.

packet filtering — The act of accepting or rejecting IP packets based on a set of rules, such as source or destination address.

passive caching — When active caching is disabled, the proxy cache service only retrieves Web pages when clients request them.

proxy array — Two or more proxy servers that function in parallel providing the caching service. A proxy array appears as one machine to the client; each server con-

tains separate cached data. A proxy array provides a load-balancing function for Web caching. If one server becomes unavailable, the other servers continue to function.

proxy chains — A group of servers or arrays that work in a hierarchical structure. One server receives a request and, if it does not have the information associated with a URL cached locally, sends the request up the chain to the next "upstream" server.

proxy server — A server hosting proxy services.

proxy service — An Application-layer gateway service that makes network connections for internal client computers and isolates a private network from an external network (most commonly the Internet). Conversely, a proxy server may restrict inbound traffic when performing reverse proxy functions.

reverse proxy — A proxy service provided to external clients accessing internal servers.

rules — Parameters by which traffic is allowed or disallowed by a filtering or proxy service.

screened subnet — A subnet protected from outside traffic by a firewall.

Socks proxy — An application-layer gateway, often considered a generic proxy, which can be used with virtually any TCP application, including Web browsers and FTP clients. Often used for services that do not have their own application proxy. In this case, the Socks proxy intercepts the packets and regenerates the packet while placing the original payload within the new packet.

spoofing — In firewalls, this term applies to the replacement of the source address in the IP header with an address that is allowed by the firewall.

stateful packet filtering (also stateful inspection) — This type of filtering maintains state information on current connections, which enables it to determine when a return connection applies to a connection established from within the network. If a return connection does not have its origins from the private network, it may be part of a hacking attempt such as a denial of service.

stateless packet filtering — This type of filtering does not retain connection information and just makes forward/drop decisions based on packet header information.

Trojan horse virus — A virus disguised as a benign program.

Web caching — Proxy Server 2.0 caches Web pages it retrieves on the behalf of clients. It then checks its cache before retrieving the data on subsequent queries from clients. If the data is in the cache, Proxy Server 2.0 provides it from the cache.

Web proxy — An application-layer gateway service that stands in for outbound connection attempts by Web browser clients, making the request to the Web server on behalf of the client and hiding the actual address of the Internal client.

WinSock proxy — An application layer gateway service that is available to clients with the WinSock proxy client installed. The WinSock proxy client can support any protocol that uses WINSock.DLL, including FTP, NNTP, Telnet, SMTP, POP3, RealAudio, HTTP, and HTTPS.

Review Questions

1. You are a network manager for a company with 10,000 desktops at 20 locations. You are in the process of adding proxy servers for control of Internet access. You are attempting to minimize individual configuration changes to the client computers when proxy server settings are modified in the future. All desktops are running Windows 98 and Windows 2000. What strategy could you use?
2. You have been hired as a consultant for a company with 270 users at one site. They presently have routed connections to the Internet using public addresses. All access is through Internet Explorer. You are helping them plan for the installation of a proxy server at their connection point to the Internet. What change will you suggest in their IP addressing?
3. Considering the scenario in the previous question, what client software would have to be added for the client computers to use the services of the proxy server?
4. Your company headquarters has a T-1 connection to the Internet and Web servers and FTP servers on the internal network for access from within the private network. They are adding a new regional office of 80 users and planning to connect that office to corporate headquarters with a 128 Kbps connection. Tests show that this should be more than adequate for their present and future needs (up to three years), even while allowing the regional office users to access the network through headquarters. You must provide secure access to the internal Web and FTP servers for the regional office clients, while providing the same for all clients accessing the Internet. Briefly describe where you would place proxy servers for this scenario and how you would configure them.
5. Consider the previous scenario; it is six months after implementing your design, and unexpected growth in the number of users and their Internet usage has resulted in complaints that Internet access is slow at both locations. What is the first change for which you will consider using Proxy Server 2.0?
   a. Create a proxy array at the regional office.
   b. Install Socks proxy client software on each client.
   c. Create a proxy array at headquarters.
   d. Use DNS round robin.
6. Microsoft Proxy Server 2.0 provides Web page caching, proxy services, IP filtering, and routing. True or false?
7. Your company has several sites with a total of 26,000 users; 8,000 are at corporate headquarters. All locations have more than 2000 clients needing Internet access, which will be provided directly from each location. You have included a proxy array in your design for all locations. What performance enhancement will the array provide for each site? Choose all that apply.

a. fault tolerance
b. IP filtering
c. Socks caching
d. Web caching

8. Proxy Server is an application that runs on NT 4.0 and Windows 2000. True or False?
9. Select all of the following that are capabilities available with Proxy Server 2.0:
   a. Internet access to authorized users through access control settings
   b. creation of screened subnets for routing between network segments
   c. Web page caching
   d. connection of dissimilar network segments
10. What is the name of the Swiss institution whose computer scientists were involved in the beginning of the World Wide Web and the first standards for Web access?
11. Select all of the following that apply to Web proxy:
   a. requires that it be installed with the Microsoft Proxy Client
   b. is the service of choice for support of IPX/SPX clients
   c. responds to Web browser requests using HTTP, HTTPS, and FTP
   d. supports Socks clients
12. What other network service would you include in a proxy server design to provide authentication of communications between sites?
13. If you wanted to add routing capabilities to a proxy server, what Windows 2000 service would you use?
14. Which of the following statements are true of NAT? Choose all that apply.
   a. NAT is a Session-layer routing protocol.
   b. NAT is more configurable than ICS.
   c. With NAT on a proxy server, you do not need to configure Proxy Server 2.0 to do IP filtering.
   d. NAT and Proxy Server 2.0 cannot be on the same network segment.
15. Which of the following are true of Proxy Server 2.0 and DNS on the same server? Choose all that apply.
   a. DNS can provide name resolution for the internal network.
   b. Proxy Server 2.0 and DNS cannot be combined on the same server.
   c. You must be sure to enable DNS service on the external interface.
   d. You can combine Proxy Server and DNS on the same server.

16. Which of the following statements are true when you are planning for multiple proxy servers? Select all that apply.
    a. The external adapter must be configured with the address of an internal DNS server.
    b. The internal adapter must be configured with the address of an external DNS server.
    c. The internal adapter must be configured with the address of an internal DNS server.
    d. The internal adapter should be configured with the address of a second internal DNS server for fault tolerance.
17. Which of the following statements are true when you are planning to include the DHCP service and proxy server 2.0 on the same server? Choose all that apply.
    a. Proxy server 2.0 and DHCP service cannot run on the same server.
    b. Proxy server 2.0 and DHCP service can run on the same server.
    c. Ensure that the internal network interface does not have a default gateway configured.
    d. Be sure that the server is also a DHCP Relay Agent.
18. If your internal network has WINS servers, what is the recommended WINS configuration for the proxy server internal adapter?
19. You are considering combining WINS and proxy services on the same server. How would you configure the gateway setting for your internal interface?
20. Which of the following are design decisions for a functional design? Choose all that apply.
    a. number of proxy arrays
    b. placement of proxy servers
    c. network interface characteristics, including IP address, persistence, data rate, and security
    d. method by which internal clients will access the proxy server

HANDS-ON PROJECTS

The following Hands-on Projects will take you through the installation and configuration of Proxy Server 2.0, and the installation of Microsoft Proxy Client.

To complete these projects, each student will need the following:

1. A Windows 2000 Advanced Server computer with two network interfaces, one "internal" and the other "external." The internal interface must be a NIC; the external interface may be a NIC or a standard or cable modem or ISDN device. Verify that the internal interface has a valid IP address and mask for the internal network and has no

other network protocols installed (IPX/SPX). Do not specify a default gateway because a route to your internal network can be created from the external network. Verify that the external interface is set up with the proper IP address information.

2. Your instructor will provide you with one of the following:
   - Microsoft Proxy Server 2.0 compact disc
   - Microsoft Back Office Server 4.0 or 4.5 disk 3
   - A network share location containing the contents of one of these disks
3. Your instructor will also provide you with the 10-digit CD key, which you will need to enter when prompted. Write it here: _____
4. You will also need Internet access from the classroom in order to complete Hands-on Project 8-1. If this is not available, the instructor will provide you with a location on the local network from which you can run the Proxy Update wizard.

In Windows 2000, if you place the insertion point over something on the screen and press F1, help for that item will appear. This is very useful for understanding all the options available in the various dialog boxes you will encounter here.

Project 8-1 Install Proxy Server

This project will take you through the installation of Proxy Server 2.0, which requires an update to run on Windows 2000. This update will be performed during the installation.

1. If you are not logged on, log on to your Windows 2000 server as **administrator** in the domain **intersales.corp**.
2. Close all open windows.
3. Open your Web browser and point to **http://microsoft.com/proxy**.
4. Click **Downloads** (near bottom of page).
5. The Download page appears. Click **Microsoft Proxy Server 2.0 for Microsoft Windows 2000**.
6. The Microsoft Proxy Server 2.0 for Microsoft Windows 2000 Download page appears. Scroll to the bottom of the page and click **Microsoft Proxy Server 2.0 Update Wizard** in the language of your choice.
7. A file download dialog box opens. Click the **Save this program to disk** option button. Click **OK**.
8. The Save As dialog box opens. Double-click **Desktop** in the Save in: selection box to highlight it.
9. Click the **Save** button to download and save the program **"msp2wizi"** (in the File name: selection box) to the desktop.
10. Click **Close** in the Download Complete dialog box.

11. Click the **Close** button in the upper-right corner of your browser window to close the browser.
12. Double-click the **msp2wizi** icon on your desktop to run the Microsoft Proxy Server 2.0 Update wizard for Microsoft Windows 2000.
13. Click **Yes** on the Supplemental End User License Agreement dialog box for Microsoft Software.
14. The Setup Wizard dialog box opens. If you are using a CD, insert it now. Click **Continue** to start the installation.
15. If you are using a network share, click **Continue**, and then select the mapped drive from the Browse for Folder dialog box. Click **OK**.
16. Click **Continue** on the Microsoft Proxy Server Setup dialog box.
17. If you are asked for it, enter the CD Key you got from your instructor in the dialog box and click **OK**.
18. The Product ID dialog box opens. Click **OK**. Setup searches for installed components.
19. The Installation dialog box opens. Click the **large button** next to Installation Options to start installation.
20. The Microsoft Proxy Server – Installation Options dialog box opens. Click **Select All** and then click **Continue**. Setup stops WWW services.
21. The Microsoft Proxy Server Cache Drives dialog box opens. When the Proxy install program defaults to Drive C as a cache drive, but it is never a good idea to use the drive that holds the operating system for Web page caching (or other such tasks). If more than one drive is listed, choose a drive other than the one that holds the operating system.
22. Enter a Maximum Size value (100 MB is reasonable for this project) in the Maximum Size box and click **Set**. The chosen cache size will appear next to the selected drive.
23. If you were able to select a drive in the previous two steps, then do this step; otherwise, proceed to the next step. If drive C holds the operating system, select **Drive C**, enter a maximum size value of **0**, and click **Set**. This will ensure that a cache is not placed on Drive C. Notice the Total Maximum Size shown at the bottom of the dialog box.
24. Click **OK** in the Microsoft Proxy Server Cache Drives page.
25. The Local Address Table Configuration dialog box opens.
26. Click **Construct Table**.
27. Ensure that a checkmark is in the check box for Add the private ranges.
28. Ensure that a checkmark is in the Load from NT Internal Routing Table check box.
29. Click the **Load known address ranges from all IP interface cards** option button.

30. Click **OK**.
31. The Setup Message dialog box appears. Click **OK**.
32. The Local Address Table Configuration dialog box reappears with addresses in the Internal IP Ranges box. Click **OK**.
33. The Client Installation/Configuration dialog box appears. Accept the default settings by clicking **OK**.
34. The Access Control dialog box opens. Accept the default settings by clicking **OK**. Note that you are enabling both WinSock proxy and Web proxy services.
35. The Setup Information dialog box opens with a message about the packet filtering security feature, which can be configured with the administration tool. Click **OK**. Setup completes the installation and starts the WWW services.
36. Click **OK** on the dialog box that states that Microsoft Proxy Server 2.0 installation was successful.

You have installed Proxy Server 2.0 using the update tool for Windows 2000, configured cache drives, configured a Local Address Table, and enabled proxy services.

Project 8-2 Configuring Proxy Server

This project demonstrates how to configure a high-security configuration between a LAN and the Internet. It assumes successful completion of Hands-on Project 8-1.

1. On the desktop display, click the **Start** button on the taskbar, point to **Programs**, point to **Microsoft Proxy Server**, and then click **Microsoft Management Console**.
2. To access the packet filter configuration, double-click your server name in the tree in the left pane.
3. Proxy Server 2.0 considers packet filters a shared service. Therefore, to access the packet filter configuration, right-click any of the **Web Proxy**, **WinSock Proxy**, or **Socks Proxy** service objects in the left pane of the MMC, and then click **Properties**. The (Chosen) Proxy Service Properties for your server page appears.
4. On the Service tab page, click the **Security** button. The Security dialog box opens. Configuration changes made on this tab affect the entire Microsoft Proxy Server.
5. To enable packet filtering, check the **Enable packet filtering on external interface** check box. This configures Microsoft Proxy Server 2.0 so that no traffic (except the packet types listed in the exceptions list) will flow between the public and private interfaces.
6. Check the **Enable filtering of IP fragments** check box so that fragments will not be allowed.
7. Notice the default settings, which allow for use of the ping command, and also allow the internal clients to receive packets signaling source quench, timeout, and unreachable host.

8. Click the **Help** button and explore the information concerning packet filters.
9. In the Packet Filters page of the Shared Services Help page, scroll down and click **Packet Filter Properties**.
10. Click each of the items in the list to better understand the options you can choose for packet filtering, and to see the explanation of the **predefined filter**. Close the Shared Services Help window.
11. Click **OK** in the dialog box, and then close the MMC.

Project 8-3 Restricting Access to External Web Sites

The Web proxy service gives network administrators the ability to restrict access to HTTP and FTP sites by name or IP address. As an example for this project, let's say we want to restrict a user named Samuel from using FTP service but grant him access to HTTP so he can access the Internet.

1. On the desktop display, click the **Start** button on the taskbar, point to **Programs**, point to **Microsoft Proxy Server**, and then click **Microsoft Management Console**.
2. Double-click your server name in the Tree tab of the left pane.
3. Right-click the **Web Proxy** service object in the left pane of the MMC, and then click **Properties**. The Web Proxy Service Properties for your server page appears.
4. Select the **Permissions** tab and check the **Enable access control** check box, if necessary. When this box is checked, you use the protocol through the proxy.
5. We want to restrict Samuel from using FTP. When access control is enabled, which we just did in Step 4, then access is only granted to users or IP addresses which appear in the window. Thus all we have to do to deny him access is to do nothing; that is, leave his name out of the window.
6. We also want to grant Samuel the ability to use HTTP. To do this, click the **Protocol** list arrow, and then click **WWW**.
7. Click the **Edit** button to access the list of users with access granted. The WWW Permissions dialog box opens.
8. In the WWW Permissions box, click **Add**. The Add Users and Groups dialog box opens.
9. Scroll down the list of users until you find Samuel (presuming, of course, that he exists on your system), click his name to highlight it, and then click **Add**.
10. Click **OK** to close the Add Users and Groups dialog box.
11. Click **OK** twice to close the two dialog boxes.
12. Samuel is now granted access to HTTP through the Web proxy but denied access to FTP.
13. Click **OK** to close the dialog box, and then close the MMC.

Project 8-4 Making the Connection with ICS

In this project, you will go through the steps to share a connection with ICS. This is a beneficial skill because you may need to do this in order to connect a small office to the Internet. You will not, however, actually complete the task of enabling ICS, because it modifies the IP address of your internal network adapter, which would disable your network access in the classroom.

1. On the desktop, right-click **My Network Places** and click **Properties**. The Network and Dial-up Connections dialog box opens.
2. Right-click the **external interface** of your computer and click **Properties**. The Properties dialog box for the public interface opens.
3. Select the **Sharing** tab. Check the **Enable Internet Connection Sharing for this connection** check box.
4. For the purposes of enabling ICS, we could simply click OK and quit now. But for the purposes of this project, we will explore this dialog box further.
5. Click the **Enable on-demand dialing** check box.
6. Click **Settings** to access the Internet Connection Sharing Settings dialog box. Note that the Applications tab allows you to list the network applications to be enabled for computers sharing this connection, and that the Services tab allows you to select the services to be provided to the remote network.
7. Click **OK** to close the Internet Connection Sharing Settings dialog box.
8. Click **OK** to close the (External Connection) Properties dialog box.
9. When the warning about connectivity with other members of the network being lost appears, click **NO** to close the message window.
10. Click **Cancel** in the Connection Properties dialog box.
11. Close the Network and Dial-up Connections window.

Project 8-5 Installing and Configuring NAT

The purpose of this project is for you to understand how to install NAT and what configuration options exist. Thus, this is partially a project and partially a tutorial.

1. On the desktop, click the **Start** button on the taskbar, point to **Programs**, point to **Administrative Tools**, and then click **Routing and Remote Access**.
2. The Routing and Remote Access MMC opens. Expand the objects in the console tree until IP Routing displays. Expand **IP Routing** so that the General node appears.
3. Right-click the **General** node, and click **New Routing Protocol**. The New Routing Protocol dialog box opens.
4. Select **Network Address Translation (NAT)** from the list, and then click **OK** to close the list and install NAT.

5. To access the configuration settings for NAT, right-click the **Network Address Translation (NAT)** object in the scope pane and then click **Properties**. The Network Address Translation (NAT) Properties dialog box opens.
6. The General tab shows the global settings for event logging. The default setting allows logging only of errors. There are two other options for variations in logging and the option to disable event logging.
7. The NAT server translates the IP address and port values in the request to forward packets. The translation data is stored in a database so that return packets can be properly mapped back to the original requesting host. The settings on the Translation tab define how long data remains in the translation database. Note the default times.

The Address Assignment tab enables the NAT server to use DHCP to automatically assign IP addresses to computers on the private network. The Name Resolution tab enables the NAT server to use a server's friendly name rather than an IP address. It allows you to choose whether to resolve IP addresses for clients using DNS and whether to connect to the public network when a name needs to be resolved. If you choose to connect to the public network, you can enter the demand-dial interface information.

8. Close the Network Address Translation (NAT) Properties dialog box. NAT is not automatically applied to an interface. You now need to choose the interfaces involved in address translation.
9. To add an interface, right-click the **Network Address Translation (NAT)** node in the scope pane, and then click **New Interface**. The New Interface for Network Address Translation (NAT) dialog box opens.
10. Select the interface that you want the routing protocol to run on. You will select at least one private and one public interface.
11. Click **OK**. The Network Address Translation Properties – (chosen interface) Properties dialog box opens. You can choose whether it is to be a private interface or a public interface. If you choose public, you can also choose whether to allow translation of TCP/UDP headers to allow other computers to send and receive data through this interface.
12. Close all open windows.

Project 8-6 Installing the Microsoft Proxy Client

In this project, you install the Microsoft Proxy Client *not* using a CERN-compatible browser *and* if you are running a WinSock application.

1. On the desktop, right-click the **Start** button on the taskbar and click **Explore**. Explorer opens.
2. Click the **plus sign (+)** on Local Disk (C:) to expand it if it is not already expanded. Note that your computer's Local Disk might be a disk other than C:.
3. Click the **plus sign (+)** on the msp (Microsoft Proxy) folder to expand it.
4. Click the **clients** shared folder to display its contents in the right pane.
5. Double-click the **Setup** program icon in the right pane. The Microsoft Proxy Client Setup dialog box opens.
6. Click **Continue**. Setup searches for installed components.
7. To start installation, click the large **button** next to Install Microsoft Proxy Client. Setup searches for disk space, installs the client software, and announces that Microsoft Proxy Client 2.0 Setup was completed successfully.
8. Click **OK**. The Setup – Restart System dialog box opens.
9. Click **Restart Windows Now**. Windows 2000 shuts down and restarts itself.
10. Log on to Windows 2000. The Explorer window will be open. Close it now.
11. On the display, click the **Start** button on the taskbar, point to **Settings**, and click **Control Panel**. The Control Panel opens.
12. Double-click the new **WSP Client** icon in the Control Panel. The Microsoft WinSock Proxy Client dialog box opens. The default setting is Enable WinSock Proxy Client. You can also force use of the IPX/SPX protocol. If your network is running only IPX/SPX and the client computer has TCP/IP installed, you should select this check box. Any changes made on the server to the WinSock Proxy Service are downloaded to the client when the Update Now button is clicked. Click **OK** to close the dialog box.
13. Double-click **Add/Remove Programs** in the Control Panel. The Add/Remove programs dialog box opens.
14. Click **Microsoft Proxy Client**. An expanded blue highlight box appears around it and a Change/Remove button appears.
15. Click the **Change/Remove** button. Install searches for installed components and the Microsoft Proxy Client Setup dialog box appears.
16. Click the **Remove All** button to remove installed components from the current installation. A Setup Message dialog box appears asking if you are sure you want to remove Microsoft Proxy Client. Click **Yes**.
17. If a message box telling you that it could not remove a program appears, click **Ignore**. Click **OK** in the resulting message box, and then click **Restart Windows Now**.
18. Log on to Windows 2000. Control Panel will be displayed. Close it.

Project 8-7 Configuring Internet Explorer 5.0 to Use an Application Gateway

In this Project, you configure Internet Explorer 5.0 to use an application gateway. This configuration is valuable in your quest to supply services to internal users.

1. On the desktop, click the **Start** button on the task bar, point to **Programs**, and then click **Internet Explorer**. If asked, enter an appropriate Network username and password.
2. On the **Tools** menu, click **Internet Options**. The Internet Options dialog box opens.
3. On the Connections tab, click **LAN Settings**. The Local Area Network (LAN) Settings dialog box appears.
4. Check the **Use a proxy server** check box. In the Address box, enter either the IP address or the DNS name of your proxy server. In the Port box, enter either 80 or the port where your proxy is configured to run. You have now configured your browser to use a proxy server.
5. Uncheck the **Use a proxy server** check box to restore Internet Explorer to non-proxy service. Close **Internet Explorer**.
6. Close all open windows.

CASE PROJECTS

Case 8-1 Designing for Basic Internet Connectivity with Proxy Server

You are a consultant hired by a fruit-packing company in California. They presently have an NT domain, with plans to upgrade to Windows 2000 Active Directory in the next eight months. Their corporate offices are in Davis, with branch offices in Modesto, Fresno, and Bakersfield. Each location requires Internet access. Davis has a T-1 connection to the Internet. All offices connect directly to Davis with 56 Kbps connections and access the Internet through Davis.

They currently have a firewall at Davis and routers at each of the branch offices, all purchased six years ago. Most desktop computers are running Windows 95 or 98, but a few Macintosh computers are used in the graphics department for label designs and they also have Internet access. You have been asked to come up with a plan to replace their connection equipment. Outline a simple design using proxy servers in place of the present firewall and routers. Include client-side configuration in your plan.

The company now has acquired a small fruit-packing company in Corcoran. They have one office with an IPX-SPX-based network with NetWare 4.*x* servers. They currently only have a few modem connections from desktops to the Internet. You have determined that a 56 Kbps connection to Davis would be adequate for this location, and if you can limit unnecessary traffic across the link, this bandwidth would most likely be more than

adequate for at least the next three years. Devise a design to connect Corcoran to Headquarters and to the Internet as soon as possible using a proxy server. What would you recommend for the Corcoran internal network?

Case 8-2 A Proxy Server Design for Security and Performance

You work for a small manufacturing company with four sites. The three remote sites presently have 56 Kbps connections to the main location. All sites also have their own Internet connections to an ISP. You have devised a plan that calls for proxy servers at each end of all WAN connections, as well as on the Internet connection points. The owner of the company has been discussing these plans with his brother-in-law, who has started working in his basement to build computers from components. The brother-in-law has read a few books on networking and TCP/IP, and he has advised your boss that your plan is too costly because you should only need proxy services on the Internet connections. Write an explanation and justification for having the proxy servers on each end of the WAN links.

Within the company, users are accessing Web servers and an FTP server in the main location as well as on the Internet. Describe how you have configured the proxy servers for better performance for client access to these servers. Further, to defend your decision and networking knowledge, explain what option you would consider to improve performance for Web proxy clients if this were a larger company with greater Internet usage.

Case 8-3 A Proxy Server Design Enhanced for Availability

XYZ Beauty Supply is headquartered in Oklahoma City with regional and branch offices in 40 states. Each location has Internet access through a single server running Microsoft Proxy Server 2.0. The number of users per site ranges from 100 to several hundred. They migrated to a single Windows 2000 Active Directory domain in January 2001.

You have been called in as a consultant and told that recently users in some of the larger sites have reported problems accessing the Internet, including a situation in which they could not access the Internet because the single proxy server at their location was down. Obviously the single-server solution is not working for all of the sites. With the information provided, what would be some possible solutions you could pursue for this client?